Amendments to the Specification

Please replace the paragraph that begins on Page 1, line 5 and carries over to Page 2, line 4 with the following marked-up replacement paragraph:

-- The present invention is related to the following commonly-assigned U. S. Patents: U. S. Patent 7,010,681 (serial number 09/240,387, filed 01/29/1999), titled "Method, System and Apparatus for Selecting Encryption Levels Based on Policy Profiling"; U. S. Patent 6,585,778 (serial number 09/385,899, filed 08/30/1999), titled "Enforcing Data Policy Using Style Sheet Processing"; U. S. Patent 6,931,532 (serial number 09/422,430, filed 10/21/1999), titled "Selective Data Encryption Using Style Sheet Processing"; U. S. Patent ~~6,961,849~~ 6,978,367 (serial number ~~09/422,537~~ 09/422,492, filed 10/21/1999), titled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Client Proxy"; U. S. Patent ~~6,978,367~~ 6,961,849 (serial number ~~09/422,492~~ 09/422,537, filed 10/21/1999), titled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Group Clerk"; U. S. Patent 6,941,459 (serial number 09/422,431, filed 10/21/1999), titled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Key Recovery Agent"; and _____ (serial number 10/455,068, filed 6/5/2003), titled "Method, System and Program Product for Limiting Insertion of Content between Computer Programs". --

Please replace the paragraph that begins on Page 28, line 13 and carries over to Page 29, line 7 with the following marked-up replacement paragraph:

-- The value of Ekey attribute 364 is an encrypted version of a symmetric key. The underlying symmetric key was used to encrypt the rules and document component of the security

container, and can therefore be used to decrypt that information for an authorized requester. According to preferred embodiments, techniques disclosed in the referenced inventions are used to create the encrypted version of the symmetric key, and a different encrypted version of that symmetric key is created for each distinct key element (e.g., as shown in the Ekey attribute of key elements 361, 371, 381), thereby securely distributing the symmetric key to each authorized entity. In particular, the public key associated with the entity whose key identifier 363 (see also element 420 of Fig. 4A) is specified in the key element 361 is used to encrypt the symmetric key, such that the entity's private key can then be used to recover the symmetric key in clear text. Therefore, referring to the key elements within key class [[300]] 301 of Fig. [[3A]] 3B, key element 361 includes (in its Ekey attribute) the symmetric key as encrypted by the public key of the managers group, key element 371 includes this same symmetric key as encrypted by the public key of an individual user (having common name "E135246" and organizational unit "users" in the DN attribute value), and key element 381 includes the same symmetric key as encrypted by the public key associated with the "hr" (for "human resources") group. --

Please replace the paragraph on Page 33, lines 2 - 7 with the following marked-up replacement paragraph:

-- It should be noted that techniques for authenticating a user, determining a user's membership in a group, providing the group's private key to the user, and performing decryption using the group's private key on behalf of the user are outside the scope of the present invention. Techniques disclosed in the commonly-assigned U. S. Patent 6,961,849 titled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Group Clerk" are one way in which

this could be done. --